Secure Mass Storage Device with Embedded Biometric Record that Blocks Access by Disabling Plug-and-Play Configuration

Abstract of Disclosure

An external mass storage device is secured against unauthorized access. A fingerprint reader is integrated on the external mass storage device. An initialization routine is executed when the device is plugged into a personal computer (PC) using a USB, IEEE 1394, PCMCIA, or other interface. The initialization routine scans the user"s fingerprint and extracts biometric information. The biometric information is compared to stored biometric records to determine if the user is authorized to access the external mass storage device. When authorization fails, the initialization routine halts, preventing the PC from mounting the external mass storage, thus blocking access. When authentication passes, initialization continues and the external mass storage is mounted and accessible from the PC. Since the initialization routine and stored biometric records are stored on the external mass storage, the external mass storage is protected even when moved to a different PC. Special biometric security software does not have to be installed on the PC.

Figures